IN THE SPECIFICATION

Kindly amend paragraph 0036 as follows:

[0036] Dependable security is of fundamental importance with accessing internal enterprise as well as personal data from remote clients. Toward achieving that end, all data sent across the network between the Connector Server and Providers is sent as compressed, serialized objects secured using standards-based encryption and authentication mechanisms. This approach is more secure than POP3, IIAP, and FTP since an ASCII-based "clear text" protocol is not used. There is no way, for instance, for a user to manually "Telnet" into a Provider 42-46 or Connector Server 30 and interact with it. ~~Dat~~ Data can also be encrypted at the device level and at the Connector server 30 so that at no point in the chain of communication between device and data store is data in an unencrypted form.

Kindly amend paragraph 0072 as follows:

[0070] As shown in FIG. 7, in a Palm Client implementation where a Palm Messaging Application 74 running on a Palm device is being supported, the API functions will be available in the Client device to higher application layers. The Messaging API software 76, which is the client side of the server software, the Inet Library 78, which controls the Palm hardware for sending data, and the Network Stack 80, which is the lower level portion of the Inet software, all run on the Palm device. Communication of the Palm device to the Connector Server 84 is through a wireless connection to the Palm wireless gateway, i.e., Elaine 82. The Connector Server 84 communicates ~~tot he~~ to the Message Store 88 through the Messaging Connector 86 which may also have as part of it a Provider as described above.